Who are the actors in a typical cybersecurity scenario?

Cybersecurity plays a crucial role in today hyper-connected world. The cybersecurity scenarios involve different knowledge actors that interact with complex Information Technology (IT) systems. The User case scenarios are a common practices for analysing requirements and developing complex software products. In addition, the aforementioned scenarios can include cybersecurity view, during the requirement analysis to tune up and meet the software product requirements. However, the threat scenarios, the cybersecurity scenarios, can adopt other models, such as STRIDE, DREAD an so on. Nowadays, the modern operators and the developers cannot adopt the threat models. In fact, a large number of the developers, operators and software managers skip the threat modelling, due to low knowledge on it and a reduced budget for the software deployment.

The low skilled developer, operator and software could introduce the thread model during the user case scenarios. However, who are the actors in a typical cybersecurity scenario? The involved actors in a typical users case scenarios could be:

- the final user, with no IT knowledge;
- the administrator, with a basic knowledge and limited knowledge on the software;
- the developer, with a limited knowledge on the software;
- the operator, with a limited knowledge on the software;
- the software delivery.

The final user can have a no IT, limited or full knowledge on the software. The final user, for a enterprise software tools, is unknown at the time of purchase. An example is a high skilled IT or hacker that buy or install a smartphone application, which can appreciate the user graphic interface, the data consuming and the software logic. The final user intensively interact with the final software product, finding a bug or asking for the improvements.

The administrator is an intermediate actor that interacts with a limited and not purchase software product views. For example, the administrator can modify the user' information, analyse the software collected data and moderate the user actions. An example is an online blog, where different users have different privileges, views and actions to update, modify, delete blog entities and blog user.

The developer and operator couldn't know all software information. The first one can know a limited information about the software products, which cannot be about the entire software product, due to the assignment of a small portion of software product tasks. The operator can also know the final software product proprieties, such as machine target, dependencies, setup and host configuration. Moreover, the aforementioned actors can have a limited background knowledge about the domain. Today, it is very simple to find and to study online a sub set of software libraries, programming language and machine proprieties. Thus, the developer and operator can learn and adapt the knowledge on an limited sub set of software components. An example is a Drupal[1] , Joomla[2] and Wordpress web developer, which learns and acquires only the knowledge about a limited software product. Furthermore, a Drupal, Joomla and Wordpress web developer can buy a custom templates and plug-ins without to know the software product process and makes beauty the own web site for selling it.

The software delivery is the unique person that has to know the software product, from economic benefits for the buyer, the limitations, security issue, bug tracks, versions and change logs. The software delivery also knows the development and deployment time.

How do the actors interact with the software product for a cybersecurity point of view? It is a hard question. First of all, the software product use case must define the

[1] https://www.drupal.org/
[2] https://www.joomla.org/

interaction actions and the sensitive information, exchanged during the its use. In general, the software product has to be resilient against the final user for incorrect input and for avoiding the exposure of sensitive information. The final user can be a low skilled user, which cannot follow the software on screen guide to fill out the software product forms. In addition, it has to be intuitive, easy to use and accessible. Conversely, the software product cannot hide its sensitive information, exposing an attack surface that a high skilled final user can exploit to compromise its. The administrator could find a bugs and can be high skilled or not. In addition, the administrator has to learn the feature of the software product for interacting with its. In conclusion, the software deliver has to take in consideration the users' and administrators' feedback and the action to mitigate the risks, informing the developers and operators about the common vulnerabilities. The final user, also the administrator, has to have a minimum background and Government should move forward to teach or prepare the population about the software risks. In fact, the phishing attack is one of the most common attacks, which can minimize if the final user is educated to avoid the click on a malicious and suspicious emails, which is not for a low skilled user and/or administrator. The software product Meanwhile, the developers and operators have to know the common vulnerabilities, for example incorrect and insecure object serialization, libraries bugs, Operating System (OS) vulnerabilities, insecure protocol, frameworks security vulnerabilities and so on. Thus, the developers and operators should keep updated about the used libraries, OS and frameworks news, meaning, they have to learn the new risks. Finally, the software delivery has to be up-to-date and learn the news about the involved IT technologies, tools, programming language and so, for introducing new approaches during the development and deployment software product stages.

Thus, the key of a good cybersecurity is not only in the software product stages. The cybersecurity is also the process to learn, teach, to be up-to-date on the new risk vulnerabilities and attack methodologies. It requires time and can be expensive. The benefits of awareness actors increases the safety of the software product. An example is the bank that informs the customers with the "daily tips" about the cybersecurity of the own bank account. Or, a Government blog or Social Media posts can inform the population about the IT vulnerabilities. In a few word, the cybersecurity is also synonym of knowledge and awareness for avoiding a trivial malicious attacks, such as phishing, malware, ransomware and virus.

Abbreviations

IT Information Technology

OS Operating System

Document History

#	Date	Description
0.1	30/03/2021	Initial version

The Information Security Group

UNIVERSITÉ DE GENÈVE

Geneva School of Economics and Management
Information Science Institute